REMARKS

The Office Action dated September 10, 2007 has been received and carefully noted. The above amendments to the specification and claims, and the following remarks, are submitted as a full and complete response thereto.

The Abstract is amended to correct informalities. Claims 1-16, 18, 19, 21, 24- 31 are amended to more particularly point out and distinctly claim the subject matter of the present invention. Support for the claims amendments is found at least in paragraph [0051]. New claims 32-36 are added. No new matter is added. Claims 1-36 are respectfully submitted for consideration.

The Office Action objected to the Abstract, stating that the language should be clear and concise and should not repeat information given in the title. It should avoid using form and legal phraseology often used in patent claims, such as, "means" and "said".

Accordingly, Applicants have amended the Abstract to comply with the requirements of MPEP §608.01(b) and 37 C.F.R. §1.72. Therefore, Applicants respectfully request withdrawal of the objection to the Abstract.

The Office Action rejected claims 1, 2, 7-10, 13-15, 23, 24, and 29-31 under 35 U.S.C. §102(e) as being anticipated by Siegel (U.S. Patent Publication No. 2004/0203799) ("Siegel"). Applicants respectfully submit that Siegel fails to disclose or suggest all of the features recited in any of the pending claims.

Claim 1, from which claims 2-9 depend, is directed to a method. Routing information is extracted from a received message at a border between a first network and a second network. At least one invalid entry is added to first-network entries of the routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network entries relate to a routing path of the message within the first network. An encrypted routing information is generated by encrypting the at least one invalid entry and the first-network entries by using an own token at least for each of the first-network entries. Routing information of the received message is replaced by the encrypted routing information. The received message is forwarded with the encrypted routing information to the second network.

Claim 10, from which claims 11-13 depend, is directed to a device. An extracting means is configured for extracting the routing information from a received message at a border between a first network and a second network. An adding means is configured for adding at least one invalid entry to first-network entries of the routing information in order to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network entries relate to a routing path of the message within the first network. An encrypting means is configured for generating an encrypted routing information by encrypting the at least one invalid entry and the first-network entries by using an own token at least for each of the first-network entries. A replacing means is configured for replacing the routing

information of the received message by the encrypted routing information. A forwarding means is configured for forwarding the received message with the encrypted routing information to the second network.

Claim 14, from which claims 15-23 depend, is directed to a method. Routing information is extracted from a received message at a border between a first network and a second network. A decrypted and reversed routing information is generated by decrypting a tokenized second-network entry relating to a routing path of the message within the second network. The content of the decrypted second-network entry is also reversed. The routing information of the received message is replaced by the decrypted and reversed routing information. The received message is forwarded with the decrypted and reversed routing information to the second network.

Claim 24, from which claims 25-29 depend, is directed to a device. An extracting means is configured for extracting routing information from a received message at a border between a first network and a second network. A decrypting and reversing means is configured for generating decrypted and reversed routing information, by decrypting a tokenized second-network entry relating to a routing path of the message within the second network, and reversing the content of the decrypted second-network entry. A replacing means is configured for replacing the routing information of the received message by the decrypted and reversed routing information. A forwarding means is configured for forwarding the received message with the decrypted and reversed routing information to the second network.

Claim 30 is directed to a device. An extractor is configured to extract routing information from a received message at a border between a first network and a second network. An adder, operably connected to the extractor, is configured to add at least one invalid entry to first-network entries of the routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network entries relate to a routing path of the message within the first network. An encryptor, operably connected to the extractor, is configured to generate encrypted routing information by encrypting the at least one invalid entry and the first-network entries, by using an own token at least for each of the first-network entries. A replacer, operably connected to the extractor, is configured to replace the routing information of the received message by the encrypted routing information. A transmitter, operably connected to the extractor, is configured to forward the received message with the encrypted routing information to the second network.

Claim 31 is directed to a device. An extractor is configured to extract the routing information from a received message at a border between a first network and a second network. A decryptor, operably connected to the extractor, is configured to generate a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of the message within the second network and further configured to reverse the content of the decrypted second-network entry. A replacer, operably connected to the extractor, is configured to replace the routing information of the received message by the decrypted and reversed routing information. A transmitter,

operably connected to said extractor, is configured to forward the received message with the decrypted and reversed routing information to the second network.

According to embodiments of the present invention, extraction of the routing information is performed at a border between a first network and a second network, wherein either at least one invalid entry is added to first-network entries of the routing information, or a tokenized second-network entry extracted from the routing information and relating to the routing path of the message within the second network is decrypted and its content is reversed. Thereby, network topology can be hidden while routing errors due to encryption of multiple names or addresses into one token can be prevented. Applicants respectfully submit that each of the above claims recites features that are neither disclosed nor suggested in Siegel.

Siegel is directed to secure network-routed voice processing in a self-contained infrastructure. Voice communications are transmitted as digitized voice packets over radio frequency links. The digitized voice packets contain one or more destination addresses in addition to other routing information. Figure 7 of Siegel illustrates a modified voice packet. The modified voice packet includes a modified header, and a voice data portion.

Applicants respectfully submit that Siegel fails to disclose or suggest at least the feature of "extracting routing information from a received message at a border between a first network and a second network," as recited in claims 1, 10, 14, 24, 30, and 31.

Siegel merely describes "border routers" 30 and 34 of a "network" 40 as illustrated in Fig. 1. However, the reference numeral "40" does not designate a "network" but is merely a transmission range with respect to a mobile communication unit (see paragraph [0025] of Siegel). Thus, the circular line in Fig. 1 of Siegel does not indicate a "border" between a first network and a second network as recited in the psently claimed invention.

Applicants further respectfully submit that Siegel fails to disclose or suggest at least the feature of "adding at least one invalid entry to first-network entries of said routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which said received message has been routed, said first-network entries relating to a routing path of said message within said first network, as recited in claim 1, and similarly recited in claims 10 and 30.

First, Applicants respectfully submit that Siegel fails to disclose or suggest an invalid entry that is added to first network entries. The modified routing information described in Siegel is not an "invalid" entry. The modified routing information merely contains new routing information changed by the router based on a new optimal path associated with the members that the router can connect to and remaining members for which the voice transmission is to be routed. Thus, the modified routing information cannot be regarded as "invalid routing information" since the modified information is used to determine future routing paths.

Second, Applicants respectfully submit that Siegel is silent with regards to the invalid entry being used to blurr or hide the actual number of routing entries. As stated above, Siegel merely describes that the modified routing information for the digitized voice packet. Thus, for at least these two reasons, Siegel fails to disclose or suggest all of the features recite in claims 1, 10 and 30.

Further, Applicants respectfully submit that Siegel fails to disclose or suggest at least the feature of "generating a decrypted and reversed routing information by decrypting a tokenized second-network entry relating to a routing path of said message within said second network and by reversing the content of the decrypted second-network entry," as recited in claim 14, and similarly recited in claims 24 and 31. More specifically, Applicants submit that Siegel is silent with regards to reversing the content of the decrypted second-network entry relating to a routing path within the second network.

Applicant further notes that this feature is not addressed in the present Office Action. Thus, in the event that the present application is not in condition for allowance, Applicants request a new non-final Office Action that addresses all of the features recited in the pending claims. For the reasons discussed above, Applicants respectfully submit that Siegel fails to disclose or suggest all of the features recited in independent claims 1, 10, 14, 24, 30 and 31.

Applicants respectfully submit that because claims 2, 7-9, 13, 15, 23, and 29 depend from claims 1, 10, 14, and 24, these claims are allowable at least for the same

reasons as claims 1, 10, 14, and 24, as well as for the additional features recited in these dependent claims.

Based at least on the above, Applicants respectfully submit that Siegel fails to disclose or suggest all of the features recited in claims 1, 2, 7-10, 13-15, 23, 24, and 29-31. Accordingly, withdrawal of the rejection under 35 U.S.C. 102(e) is respectfully requested.

The Office Action rejected claims 3 and 16 under 35 U.S.C. §103(a) as being obvious over Siegel, in view of Partanen, et al. (U.S. Patent No. 6,888,828) ("Partanen"). The Office Action took the position that Siegel disclosed all of the features recited in these claims except providing said routing header comprising a record-route header of a session initiation protocol message and a service-route header as specified for the session initiation protocol. The Office Action relied on Partanen to cure these deficiencies. However, Applicants respectfully submit that Partanen is not available as prior art against the present application in a rejection under 35 U.S.C. 103(a).

The present application has a priority date of October 21, 2003 and is owned by Nokia Corporation. Partanen, which is also owned by Nokia Corporation, issued as a patent on May 3, 2005 and has a filing date of October 2, 2001. Thus, Partanen qualifies as prior art only under 35 U.S.C. 102(e). However, according to 35 U.S.C. 103(c), prior art that qualifies only under 35 U.S.C. 102(e), cannot be used in a rejection under 35 U.S.C. 103(a) against a commonly owned application.

Accordingly, Applicants respectfully submit that the present application and Partanen were, at the time the present invention was made, owned by, and subject to an obligation of assignment to, Nokia Corporation. Thus, Partanen is not available as prior art against the present application in a rejection under 35 U.S.C. 103(a). Accordingly, withdrawal of the rejection under 35 U.S.C. 103(a) is respectfully requested.

The Office Action rejected claims 4-6, 11, 12, 17-19, 25, and 26 under 35 U.S.C. §103(a) as being obvious over Siegel, in view of Westman (U.S. Patent Publication No. 2004/0088419 A1) ("Westman"). The Office Action relied on Westman to cure the deficiencies of Siegel. However, However, Applicants respectfully submit that Westman cannot be used as prior art against the present application in a rejection under 35 U.S.C. 103(a).

The present application has a priority date of October 21, 2003 and is owned by Nokia Corporation. Westman, which is also owned by Nokia, was filed (as a PCT) on April 2, 2002 and was published on May 6, 2004. Thus, Westman qualifies as prior art only under 35 U.S.C. 102(e). However, according to 35 U.S.C. 103(c), prior art that qualifies only under 35 U.S.C. 102(e) cannot be used in a rejection under 35 U.S.C. 103(a) against a commonly owned application.

Accordingly, Applicants respectfully submit that the present application and Westman were, at the time the present invention was made, owned by, and subject to an obligation of assignment to Nokia Corporation. Thus, Westman is not available as prior

art against the present application in a rejection under 35 U.S.C. 103(a). Accordingly, withdrawal of the rejection under 35 U.S.C. 103(a) is respectfully requested.

As stated above, new claims 32-36 are added. Applicants respectfully submit that each of claims 32-36 recites features that are neither disclosed nor suggested by Siegel.

Applicants respectfully submit that each of claims 1-36 recites features that are neither disclosed nor suggested in Siegel. Accordingly, it is respectfully requested that each of claims 1-36 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

David E. Brown
Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DEB:dlh

Enclosures: Additional Claim Fee Transmittal